Assignment 4 Question 4

You need to derive the update formula for u_k so that given a kth order approximation $U^{(k)}$ satisfies $f\left(U^{(k)} + u_k x^k\right) = 0 \bmod x^k$ where $f(u) = a - u^2$. The derivation is the same as for the linear p-adic lifting. The value is

$$u_k = \left(\left(\frac{e_k}{x^k} \right) \cdot (2 \cdot u_0)^{-1} \right) \bmod x \quad \text{where } e_k = \left(a - u^{(k)}\right)^2 .$$

Now notice that dividing e_k by x^k and then reducing mod x is simply extracting the coefficient of e_k of x^k.

```
> XadicSqrt := proc(a,x::name,u0::integer,p::prime,B::posint)
  local u,d,k,e,c,uk;
      if Rem(a-u0^2,x,x) mod p <> 0 then error "invalid input u0", u0
  fi;
      u := mods(u0,p);
      d := 1/(2*u0) mod p;
      for k from 1 do
           print(evaln(u[k]) = `if`(k=1,u,uk));
           e := Expand(a-u^2) mod p;
           if e=0 then return u fi;
           if k>B then return FAIL fi;
           c := coeff(e,x,k);  # (e/x^k) mod x
           uk := mods(c*d,p); # symmetric range
           u := u + uk*x^k;
      od;
  end:
```

```
> p := 101;
  a := 81*x^6+16*x^5+24*x^4+89*x^3+72*x^2+41*x+25;
  u0 := 5;
```

$$p := 101$$

$$a := 81\,x^6 + 16\,x^5 + 24\,x^4 + 89\,x^3 + 72\,x^2 + 41\,x + 25$$

$$u0 := 5$$

The degree bound for B should be deg(a)/2 = 3 because the sqrt(a(x)) must have degree deg (a)/2.

```
> B := degree(a)/2;
```

$$B := 3$$

```
> s := XadicSqrt(a,x,u0,p,B);
```

$$u_1 = 5$$

$$u_2 = -6$$

$$u_3 = 44$$

$$u_4 = -9$$

$$s := -9\,x^3 + 44\,x^2 - 6\,x + 5$$

Check that $\sqrt{a} = s$.

```
> Expand( a-s^2) mod p;
```

$$0$$

```
> a := 81*x^6+46*x^5+34*x^4+19*x^3+72*x^2+41*x+25;
```

$$a := 81\,x^6 + 46\,x^5 + 34\,x^4 + 19\,x^3 + 72\,x^2 + 41\,x + 25$$

```
> XadicSqrt(a,x,u0,p,3);
```

$$u_1 = 5$$

$$u_2 = -6$$

$$u_3 = 44$$

$$u_4 = -16$$

FAIL

So in this case $\sqrt{a}$ is not a polynomial in $\mathbb{Z}_p[x]$. We can check by factoring in Maple

```
> Factor(a) mod p;
```

$$81\,(x + 76)\,(x^3 + 41\,x^2 + 97\,x + 69)\,(x^2 + 12\,x + 98)$$